

## Come funziona l'ARP Poisoning

ARP (Address Resolution Protocol) Poisoning è un attacco in cui un aggressore modifica in modo fraudolento le tabelle ARP di una rete locale. Le tabelle ARP associano gli indirizzi IP agli indirizzi MAC dei dispositivi connessi alla rete. L'attaccante invia pacchetti ARP falsificati alla rete, convincendo i dispositivi nella rete a associare l'indirizzo MAC dell'attaccante con l'indirizzo IP di un'altra macchina legittima. Questo consente all'attaccante di intercettare o modificare il traffico destinato alla macchina bersaglio.

## Sistemi vulnerabili ad ARP Poisoning

Tutti i sistemi che utilizzano ARP per la risoluzione degli indirizzi IP possono essere vulnerabili ad ARP Poisoning. Questo include praticamente tutti i sistemi operativi moderni, come Windows, Linux, macOS, e dispositivi di rete come router, switch e access point.

## Modalità per mitigare, rilevare o annullare ARP Poisoning

1. **Mitigazione dell'ARP Poisoning:**
  - **Static ARP entries:** Configurare manualmente le tabelle ARP su dispositivi critici con voci statiche per prevenire falsificazioni.
  - **ARP spoofing detection tools:** Utilizzare strumenti di rilevamento ARP come arpwatch, ArpON, XArp, o funzionalità integrate in alcuni firewall per monitorare e rilevare attacchi ARP.
2. **Rilevamento dell'ARP Poisoning:**
  - **Monitoraggio delle tabelle ARP:** Monitorare regolarmente le tabelle ARP per rilevare discrepanze o duplicati.
  - **IDS/IPS:** Utilizzare sistemi di rilevamento e prevenzione delle intrusioni che includano firme per ARP Poisoning.
3. **Annullamento dell'ARP Poisoning:**
  - **Flush delle tabelle ARP:** In alcuni casi è possibile ripulire o ripristinare le tabelle ARP per eliminare voci falsificate.
  - **Blocco degli attacchi:** Configurare regole nei firewall per bloccare il traffico ARP sospetto.

## Commento sulle azioni di mitigazione

- **Efficacia:** Configurare voci ARP statiche e utilizzare strumenti di rilevamento ARP possono ridurre significativamente il rischio di successo di un attacco ARP Poisoning. L'implementazione di tali misure può aiutare a proteggere la rete e i dispositivi connessi.
- **Effort per l'utente/azienda:** Configurare voci ARP statiche richiede una gestione accurata delle configurazioni di rete, soprattutto in reti di grandi dimensioni. L'installazione e la configurazione degli strumenti di rilevamento ARP potrebbe richiedere un investimento di tempo per l'installazione e la configurazione iniziale, oltre che per la supervisione continua. Tuttavia, considerando la sicurezza della rete, gli sforzi sono generalmente giustificati.

In conclusione, ARP Poisoning rimane una minaccia significativa per la sicurezza delle reti locali. Implementare misure di sicurezza proattive come configurazioni ARP statiche e strumenti di rilevamento è cruciale per mitigare il rischio di attacchi ARP Poisoning e proteggere le comunicazioni di rete da intercettazioni e manipolazioni non autorizzate.